Comments submitted on behalf of the Information Technology Association of America Election Technology Council to the members of the State of California Senate Committee on Elections, Reapportionment and Constitutional Amendments

February 8, 2006

This testimony is being provided on behalf of the ITAA and its Election Technology Council (ETC). The ITAA is one of the nation's oldest and largest trade associations for the information technology industry, representing approximately 350 companies. The ETC consists of companies which offer voting system technology hardware products, software and services to support the electoral process. These companies have organized as an association to work together to address common issues facing our industry. Current members of the ETC are: Advanced Voting Solutions, Danaher Guardian Voting Systems, Diebold Election Systems, Election Systems & Software, Hart InterCivic, Perfect Voting System, Sequoia Voting Systems, and UniLect Corporation. Membership in the ETC is open to any company in the election systems marketplace. Our members employ over 2,000 dedicated citizen employees, who all work hard to support the success of American elections.

The ETC is pleased to respond to your request for vendor perspective on issues surrounding the procurement and implementation of "open source" software products by the State of California and its county registrars.

"Open source" software has become a topic of great interest in the press and among policymakers. Considered a "passing fad" by some, extravagant claims are made both in favor and against its growing role in the software marketplace. Extreme views miss the mark. Rather than a passing fad, open source software – both as a type of software and as a software development and licensing model – is an emerging business reality that information technology (IT) customers and companies are working to address and understand. ITAA believes it is appropriate to address this subject in a balanced way, addressing the various issues involved, while leaving the rhetoric to the advocates of one cause or the other. The better course is to look at the practical, pragmatic issues surrounding

the emergence of this software development model in the marketplace, and place them in the proper context – in this case the elections and voting systems environments of the State and Counties of California.

ETC members urge the Committee to consider the very important implications of the following questions and issues in considering procurement of open source software, or applying source code disclosure requirements to systems already in use in the State.

Is There a "Greater Public Good" Involved in the Use Of Open Source Software?

To some, the development and use of open source software is part of a "movement", with philosophical and social ramifications as well as economic implications in the marketplace. To many others, open source software and its development simply provides different business models for effective competition and different revenue streams from, for example, the growing commercial market for the care and maintenance of Linux code.

ITAA believes that a pragmatic approach, focused on the practical and economic implications of open source software and its development provides a more productive ground for discussion than do the philosophical ramifications of social movements. We believe the pragmatic approach is becoming more prevalent as open source software is developed in more commercial contexts and finds its way into mainstream commercial applications, both in the enterprise and in retail markets.

Is Open Source Software, or a Mandate to Disclose Source Code for Public Review, Necessary or Appropriate in the Election Systems Environment?

New and improved voting technology has made the election process easier, more accessible, and more secure. These enhancements benefit election administrators and voters, and encourage participation in our democracy. As technology has evolved, so, too, have procedures that ensure voting equipment deployed on Election Day is reliable, accurate, and secure. Federal and state certification performed under the Independent Testing Authority (ITA) process is comprehensive, rigorous, and objective. The testing and review processes currently in place allow all authorized certification officials with a valid need to examine the software in a voting system to inspect that software. Such inspection is part of the established federal and state regimen of testing and certification for voting systems, which takes into account the election environment in which the system operates.

Several states have considered source code review or disclosure requirements for voting systems. Our Election Technology Council members believe that these proposals are ill-advised. Review by, or disclosure to, the general public

will not improve the efficiency or effectiveness of voting systems software inspection. Additional inspection and review of code by technical laypersons, with no ability to provide regulated feedback into the state election management process, is unlikely to improve the quality or security of the software.

The implementation of a requirement or preference for open source software or source code disclosure may create additional unforeseen election systems procurement and management challenges. One state which passed such a requirement into law has encountered great difficulty in conducting a voting systems procurement, as vendors were unable to provide the state with access to source code for most of the third-party software incorporated in their systems.

Further, California's use of federal and state certification processes and pre-election testing would make the discovery through public review of any software anomalies in the final weeks leading up to an election an almost unmanageable situation. The state and its counties would be faced with hard choices between remedying the problem and seeking recertification on a fast-track basis, which at this time is infeasible under current ITA practices, or running an election with known and publicized software anomalies.

How is IT Security Affected by Proprietary Software or Open Source Software?

Open source advocates and proprietary developers make various claims about the security implication of their development models. Open source advocates say that the "open community" development model encourages many more individuals to study the code and search for, find, and correct vulnerabilities. This leads to a belief that open source is actually more secure than proprietary code, because so many programmers may review the code for vulnerabilities and then add security patches to close breaches they have found. It has also been argued, however, that this openness allows for malicious hackers to review the source code and develop strategies to breach security restrictions or create their own security breaches that are difficult to detect.

It is worth emphasizing that the correct security question for voting software itself has less to do with development models and more to do with the quality of code, and whether it is more or less carefully written and developed. Quality code can be developed under both models. All code should be subjected to security evaluation and review. Moreover, software quality is only one of many important security considerations that need to be taken into account in the voting environment. A single-minded focus on technology hardware and software ignores the reality that security remains a combination of product and process, relying on informed administrators, sufficient user training, as well as various security technologies and conditions of access to voting systems. Press reports highlighting vulnerabilities of one type of software, or demonstrating "hacks" performed under laboratory conditions rather than in the election environment,

oversimplify the issue and serve no purpose other than undermining public confidence in American voting administration and systems.

Would California Election Security be Affected by the Use of Open or Disclosed Source Software?

There is no experience in the United States with the use of open source software, or disclosed source code, in the conduct of public elections. Hence, we cannot provide a case-based analysis of this question. However, scenarios can be drawn in which a motivated intruder, armed with an advanced level of knowledge of system source code, would be able to do far more harm to a voting system than an intruder possessing more limited awareness of voting system operations.

What are the Intellectual Property Concerns around an Open Source or Source Code Disclosure Requirement for Technology Companies?

Software is mostly copyrightable expression (just as is a book, movie or music) and, as such, it is subject to the protections and limitations of intellectual property under the copyright law.[1] Similarly, software source code, like many other written works (e.g., customer lists, secret formulas for products, strategic plans for future competition and an almost infinite variety of similar materials) can be protected against unauthorized disclosure under state trade secrets laws and with contractual non-disclosure agreements. Like other "written works", software is also a form of "protected speech" covered by the First Amendment. But the courts have held for a long time that there is no conflict between the free speech clause of the First Amendment, trade secret protection against unauthorized disclosure, and the Constitutional clause granting certain restrictive distribution and other copyright rights to authors for a "limited" period of time. Authors of software are entitled to the same intellectual property protection as authors of other forms of copyrightable expression subject to trade secret protection.

Most technology companies rely on a broad range of intellectual property protections, including trade secret, trademark, copyright and patent protection. Over time the software industry has come to rely on intellectual property rights to promote an atmosphere of innovation, to create an environment for sustainable businesses, and one that provides incentives to encourage firms to invest substantial resources to create new products. In the voting systems market, the investments made are not just made in the development of software code, but in the time and labor intensive processes of product testing and certification, marketing and procurement responses, and servicing products that must remain in operation in the field for a decade or more.

[1] It may be possible to describe a patentable invention solely in terms of software, giving rise to so-called "software patents", but that is beyond the scope of the present discussion.

Both the proprietary development model and the open source development model rely on copyright law as the foundation for the allocation of rights under various license agreements. To create a sustainable, profitable business, and prevent the erosion of their market-share through widespread re-use or redistribution of their core assets, it is inevitable that all enterprises will turn to copyright and trade secret protection. This is already taking place in the open source software and open standards marketplaces as technology firms seek a profitable foothold in those businesses.

ITAA holds that all software development and licensing models have a place in the software marketplace. Companies should be allowed to focus their energies and compete vigorously in the marketplace of innovation with the "best" products winning.

What are the Procurement Implications of Open Source Mandates or Preferences?

Since the late 1990's, governments at many levels here and internationally, have considered changing their public sector procurement laws to give preference to the open source development model by either creating barriers to acquisition of commercial software (or preferences for acquisition of open source software) or making the purchase of commercial software by government outright illegal. The United States government opposes such restrictions, as does the Free Software Foundation, an established advocate of open source software.

ITAA opposes government-mandated preferences at any level. Governments, like all potential and existing customers, should choose software on a technology-neutral and vendor-neutral basis, examining the merits of the technology, it advantages and its total cost, not by setting a preference for one type of software, or banning another, based on its licensing or development model.

Certain systems acquisitions may depend to a greater or lesser degree on issues of cost, quality, standardization, security requirements, or a universe of other factors that may lead a customer to prefer a certain type of software. A blanket policy can never capture these many nuances and can never allow a competent software buyer to effectively weigh all factors.

ITAA encourages a "best value" analysis, including consideration of the total cost of ownership when acquiring an IT solution, including the cost of implementation, testing and maintenance expense, as well as the benefits of adding new system capabilities to increase customer flexibility and value. This type of analysis provides the framework for the majority of US Federal and State government information technology procurements. State policy that sets an open source software mandate or preference for voting systems procurements should be

carefully considered, as it may present a precedent for other types of California IT procurements.

Concluding Remarks

In providing this testimony, our intention is to give feedback to the Committee on the consequences of the issues under consideration to the vendor community and, as we see it, to the state and its election jurisdictions – our valued customers whom we serve.

Above all, we are responsive to customer needs and are committed to providing safe, secure, accurate, reliable and accessible voting systems. We are all involved in this process together, and by working together we can improve the process of voting, voter access and participation.

Thank you for your attention to our concerns.